

Weekly Report

June 9, 2019

1 Work

1. Unpaired Image Generation任务，之前用于做图片增强效果不佳，换了Sketch to Image的任务后，生成的图片的效果也不太好。
2. Adversarial Attack使用字典直接学习对抗样本，目前进攻的结果不够真实。
3. Unsupervised Representation Learning，基于无监督学习的方法学习图片特征，可以用于Classification等任务。即将开始这个任务，目前在看一些state-of-the-art的文章。
4. 工作时长：工作日每天10个小时，周末共10个小时，共60小时。

1.1 工作进度

Table 1: 工作进度

项目	进度	截止时间
DRGraph	正在修改代码	6.30
Unpaired Image Generation	目前初步的实验效果不佳	7.30
Universal Flow Attack	基于字典学习Adversarial Attack	6.30

2 Paper Reading

2.1 Things You May Not Know About Adversarial Example: A Black-box Adversarial Image Attack

虽然目前对抗样本的效果很好，但是大部分的对抗样本是在连续空间计算的，一旦返回到RGB离散空间进攻效果就会失效。本文首先调研了目前的进攻算法，发现

大部分算法都会受到影响。本文提出不基于梯度的优化方法，首先随机生成一系列 candidates，然后选取效果最好的 candidate 继续生成一些相似的样本。

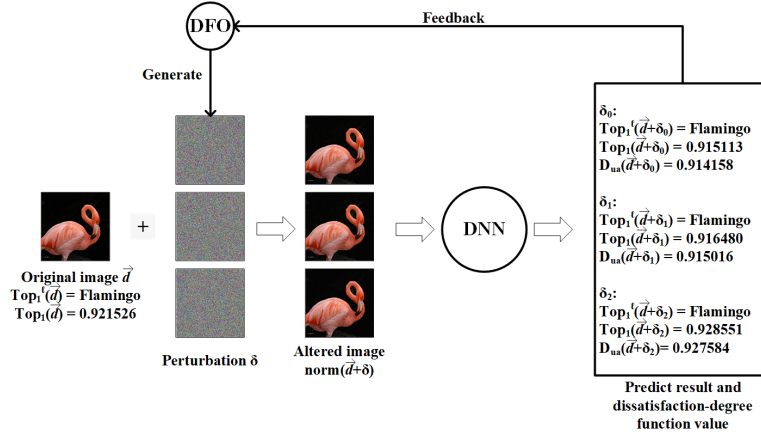


Figure 1: #1

2.2 KGAT: Knowledge Graph Attention Network for Recommendation

传统的推荐方法聚焦于user和item之间的联系，本文提出引入知识图谱，加强item和item之间的相关性，则推荐任务可以看做是在知识图谱上的推荐任务（把user和item也加入到knowledge graph中）。首先使用TransR把graph进行投影，然后采用图卷机和注意力机制，迭代生成新的node的representation，最终讲user和item对应的向量的乘积作为预测值。

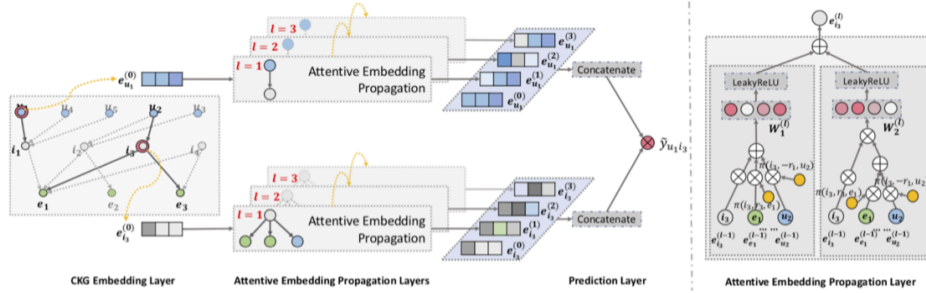


Figure 2: #2

2.3 Inductive Representation Learning on Large Graphs

一篇早期的图神经网络的文章。这里的定义其实和CNN是类似的，CNN的可以看做是对每个像素及其领域的像素特征的聚合，如果把像素及其领域看做是graph中的节点和相邻节点，就可以把GNN和CNN联系起来。每一层GNN的作用是重新计算节点的特征（结合它邻居的属性），这里往往是把邻居的属性做avg，max，或者mean（因

为graph中邻居数量不定，无法采用权重求和），然后把这个向量乘以一个权重，加偏置，输入到激活函数。多层连接起来就可以构造出一个GNN，然后最后一层的feature可以用来求相似性。



Figure 3: #3

2.4 LEARNING DEEP REPRESENTATIONS BY MUTUAL INFORMATION ESTIMATION AND MAXIMIZATION

本文主要是用于非监督的方式学习特征，主要不同是loss的目标选取的是mutual information（主要是用来判断两种分布是否接近），也就是原始图片的分布是否和特征的分是相关的（不相关的话，互信息为0）。

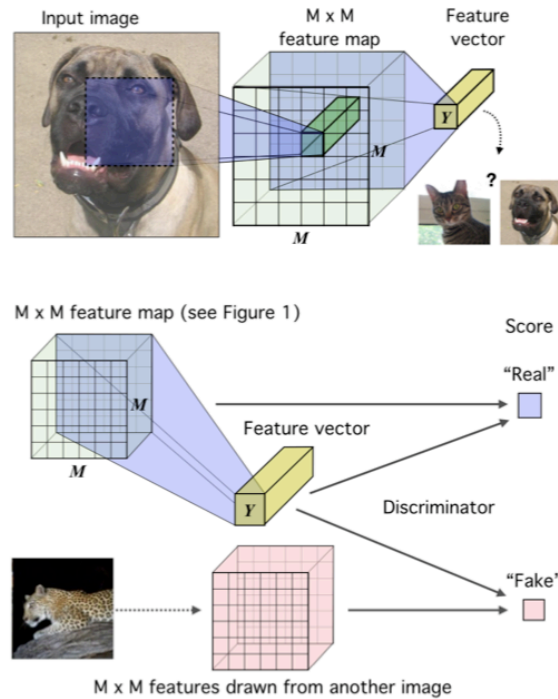


Figure 4: #4